DEPARTMENT OF THE AIR FORCE
HQ AIR INTELLIGENCE AGENCY

AIR INTELLIGENCE INSTRUCTION 33-203

22 AUGUST 2000

Communications and Information

THE AIR INTELLIGENCE AGENCY TEMPEST AND EMISSION SECURITY PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AIA WWW site at: http://pdc.aia.af.mil.

OPR: 690 ISS/PI-T
(Mr. David Conovaloff)
Certified by: 690 IOG/CC
(Colonel Gilly A. Marshall)
Supersedes AFICR 56-16, 15 April 1992.
Pages: 30
Distribution: F

This instruction implements AFPD 33-2, *Information Protection*, AFI 33-203, *Emission Security (EMSEC)*, and the national TEMPEST program for Sensitive Compartmented Information Facilities (SCIF) in the Air Intelligence Agency (AIA). It establishes procedures to control compromising emanations (CE), identifies NONSTOP countermeasures (CM), and prevents HIJACK hazards. It brings AIA into compliance with the revised national and Department of Defense (DoD) TEMPEST policies. It requires compliance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300, *National Policy on Control of Compromising Emanations*, and Department of Defense Directive 5200.19, *Control of Compromising Emanations (C)*. This TEMPEST instruction and criterions applies to HQ AIA and AIA subordinate units worldwide which operate, maintain, and install systems and equipment used to process National Security Information (NSI). This instruction also applies to AIA gained Air National Guard and Air Force Reserve units and Individual Mobilization Augmentees. This instruction does not apply to AIA activities whose non-AIA hosts provide TEMPEST or technical security. Contact your host's security officials for guidance. Direct questions and comments on the contents of this instruction through appropriate command channels to the 690th Intelligence Support Squadron (690 ISS)/PI-T, 102 Hall Blvd, Ste 145, San Antonio TX 78243-7055.

SUMMARY OF REVISIONS

This is the initial publication of AIAI 33-203. It substantially revises AFICR 56-16, *Control of Compromising Emanations (TEMPEST)*.

Chapter 1

INTRODUCTION

1.1. The AIA TEMPEST Program. This instruction describes AIA's TEMPEST program related to the Air Force, the National Security Agency, Central Security Service (NSA/CSS) Service Cryptologic Element (SCE) and the Defense Intelligence Agency (DIA). AIA, as a Field Operating Agency (FOA) and a SCE of the NSA/CSS, adopts applicable portions of DoD, USAF, DIA, and NSA/CSS documents to conduct the AIA's TEMPEST program. The national policy is contained in Director of Central Intelligence Directive (DCID) 1/21, *Security Policy for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), Security Policy Manual*, the National Security Telecommunications and Information Systems Security Policy (NSTISSP) 300, *National Policy on Control of Compromising Emanations*, and the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7000, *TEMPEST Countermeasures for Facilities (C)*. The DoD TEMPEST program is contained in DoD Directive 5200.19, *Control of Compromising Emanations (C),* and DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual.* The Air Force policy is contained in AFI 33-203, *The Air Force Emission Security (EMSEC) Program*. Portions of these documents are paraphrased or referred to throughout this document. Note: The AF EMSEC program is for collateral information and facilities only. See AFI 33-203, paragraph 12.13, for guidance for AIA facilities.

1.2. The AIA TEMPEST Philosophy:

1.2.1. Perimeter Protection. The prime objective of the TEMPEST program is to control or contain any information bearing electromagnetic emanations coming from any information processor within an AIA facility. These emanations or TEMPEST signals are a function of the TEMPEST characteristics of processing equipment, the way the equipment is installed, the electromagnetic and physical characteristic of the facility, and the geographical environment where the facility is located. As long as these signals are contained within a controlled area or the Inspectable Space, there should not be a TEMPEST problem.

1.2.2. Inspectable Space (IS). IS is defined as the 3-dimensional space surrounding equipment that processes classified and, or sensitive information within which TEMPEST exploitation is not considered practical or legal authority to identify and, or remove a potential exploitation exists. The IS may be the base perimeter, a fence around the facility, a building, or a room in a building. The means of escape may be spatial radiation, phone lines, power lines, a transmitter, etcetera. As long as all means of escape are controlled or protected at the perimeter, the area is TEMPEST secure. The IS is determined by the SCIF Accreditation Authority's Certified TEMPEST Technical Authority (CTTA). The perimeter of most bases in the continental United States (CONUS) is considered its IS.

1.2.3. TEMPEST Zone Testing. In cases where you have very limited IS or you are unsure of the amount of protection needed, TEMPEST zone testing could provide some assurance. The TEMPEST Zone Concept considers not only the free space attenuation inherent to the facility's IS, but also the attenuation provided by the physical building structure. This approach requires radio frequency (RF) attenuation measurements be performed to characterize each facility. Subsequent interpretation of the attenuation data according to prescribed criteria allows the partitioning of the facility by zone designations. Once a facility has been "zoned," the zone assignments may be used in conjunction with TEMPEST test data to assure existing equipment and systems are appropriately located, and future

equipment and systems are designed and built to appropriate TEMPEST requirements. This concept has proven to be extremely effective. Not only has increased flexibility and substantial savings been realized, but most importantly, field testing has shown that facilities using the zoning concept have become increasingly more "TEMPEST Secure." However, zoning accounts only for spatial radiation. Conducted emanations must also be considered.

1.2.4. Good Engineering and Installation Practices. Although the term is nebulous, these installation practices are the basis of a RED/BLACK installation. Good engineering and installation practices are those which provide neat, clean, and orderly installations; protect cabling from inadvertent physical damage; provide a degree of wireline accountability; and enhance the electronic security of AIA activities.

1.2.5. Separation Distances in National Policy. The separation distances in national policy (NSTISSAM TEMPESt/2-95) when used in a SCIF are based on RED/BLACK signal lines having one overall shield and are to be used as a minimum. If a separation is not specified, it is AIA's policy to maintain a minimum of 20 inches or 50 centimeters between any RED processor and BLACK equipment or copper signal lines to ensure there is not any physical contact or mutual conduction that would cause a hazard. Contact the AIA TEMPEST officer if this is not possible.

1.2.6. Recommended Method of Signal Distribution. Fiber optic cable is the recommended method of signal distribution in AIA SCIFs. It is AIA policy to migrate circuits that lend themselves to fiber optic cable to do so. This is based on TEMPEST requirements and future requirements for greater data rates requiring larger bandwidths.

Chapter 2

HEADQUARTERS FUNCTIONS

2.1. Authority. The Commander, Air Intelligence Agency (AIA/CC) retains the authority to accept the TEMPEST risk for all AIA facilities.

2.2. Directorate of Information Operations (AIA/DO). The Architecture and Integration Branch (AIA/DOXA) through the 690 Intelligence Support Squadron, Information Protect flight (690 ISS/PI-T):

2.2.1. Manages the TEMPEST program for AIA.

2.2.2. Interprets national and Air Force policy and guidance for AIA.

2.2.3. Provides technical guidance for installing AIA mission and mission support equipment.

2.2.4. Provides guidance to the Directorate of Plans and Requirements (AIA/XP), Directorate of Logistics Contracting Division (AIA/LGC), the 690th Information Operations Group (690 IOG), and the 668th Logistic Squadron (668 LS) on TEMPEST requirements for new system acquisitions, installations, and upgrades.

2.2.5. Evaluates 668 LS projects, contractor installation, and in-house projects for HQ AIA and AIA units to ensure they meet AIA TEMPEST criterions.

2.2.6. Sends recommendations for the acceptance of the risk of a TEMPEST hazard through the AIA/DO to the AIA/CC for approval or disapproval based on implementation of NSTISSI No. 7000 and the Inspectable Space Determination, and include recommendations for corrective action.

2.2.7. Visits AIA units and conducts TEMPEST workshops to train new TEMPEST officers and informs current officers of the latest changes in TEMPEST policies and practices.

2.2.8. Reviews and coordinates on System Security Plans to ensure TEMPEST compliance.

2.3. Directorate of Logistics (AIA/LG). Within AIA/LG:

2.3.1. The Electronic Systems Management Branch (AIA/LGMY) ensures AIA mission systems and equipment are adequately maintained to protect their TEMPEST integrity.

2.3.2. The Maintenance Management Branch (AIA/LGMM):

2.3.2.1. Processes all TEMPEST modification requests for systems and equipment and ensures the approved modifications are accomplished on AIA equipment in a timely manner.

2.3.2.2. Responsible for including TEMPEST considerations in logistics support planning for all acquisition programs through the delivery and Initial Operational Capability (IOC) phase of a system equipment acquisition.

2.3.3. The Contracting Division (AIA/LGC) reviews and monitors AIA contracts to ensure the requesting activity has included TEMPEST criterions when appropriate and the contractor has met these TEMPEST requirements.

2.4. The Directorate of Plans and Programs (AIA/XP). Within AIA/XP:

2.4.1. The Civil Engineering Division (AIA/XPC) coordinates with 690 ISS/PI-T on all new systems, facility upgrade requirements, designs and new construction that impact on TEMPEST criterions.

2.4.2. The Strategic Planning Division (AIA/XPX):

2.4.2.1. Ensures all AIA policies, directives, and projects consider potential TEMPEST requirements through coordination with 690 ISS/PI-T.

2.4.2.2. Coordinates with 690 ISS/PI-T on support agreements where TEMPEST is involved.

2.5. The Security Office (AIA/SO):

2.5.1. Coordinates with 690 ISS/PI-T on all TEMPEST accreditation matters, technical security reports, and surveys for AIA-sponsored SCIFs.

2.5.2. Coordinates with 690 ISS/PI-T on physical security matters as they pertain to TEMPEST within the criterions in DCID 1/21 and DoD 5105.21-M-1.

2.6. AIA and AIA-Collocated Units. HQ AIA directorates and major staff offices and AIA-collocated units on Security Hill, including Joint Intelligence Operations Center (JIOC), Cryptologic Support Group (CPSG), Air Force Information Warfare Center (AFIWC) and their respective buildings and facilities:

2.6.1. Appoints a TEMPEST functional representative to assist the 690th Support Squadron (690 SPTS) TEMPEST officer. These functional representatives must send their names, ranks, office symbols, and telephone numbers to the Commander (690 SPTS/CC) and an information copy to 690 ISS/PI-T.

2.6.2. Each functional representative assists in the yearly RED/BLACK TEMPEST inspection and is responsible for initiating corrective action on any documented discrepancies.

2.6.3. Follows the TEMPEST security program developed and implemented by the 690 SPTS.

2.6.4. Individual project offices coordinates TEMPEST requirements directly with the AIA TEMPEST officer in the 690 ISS/PI-T for mission systems.

2.6.5. The AIA TEMPEST officer or the 67 SPTS TEMPEST officer signs the AF Form 3215, **Communications Systems Requirements Document**, AF Form 332, **Base Civil Engineering Work Request,** work orders for contracts, and self help projects requiring TEMPEST criterions.

2.7. 690 SPTS TEMPEST Officer through 690th Intelligence Support Squadron (690 ISS/PI-T):

2.7.1. Develops, implements, and conducts the AIA TEMPEST annual RED/BLACK inspection for units on Security Hill. This may be accomplished throughout the calendar year. TEMPEST deficiencies are to be identified, documented and monitored for correction, send information copies to 690 ISS/PI-T. Use AIACL 33-1 for this inspection.

2.7.2. Reviews AF Form 3215, AF Form 332, and self help projects requiring TEMPEST criteria.

2.8. Engineering and Installation. The 668 LS ensures that all 668 LS-installed mission and information systems at AIA facilities comply with this TEMPEST criterion.

2.9. Maintenance. The 690 ISS ensures that all mandatory TEMPEST modifications to telecommunication and COMSEC equipment are performed, TEMPEST corrective actions are

implemented as required, all telecommunications programming documents encompass TEMPEST criterions as appropriate, and TEMPEST policies and procedures are incorporated into COMSEC annexes to plans.

Chapter 3

UNIT RESPONSIBILITY

3.1. AIA Units. The AIA unit commander will appoint a TEMPEST officer and send the officer's or noncommissioned officer's name, rank, office symbol, duty Air Force specialty code (AFSC), DEROS/ DOS, DSN and NSTS telephone numbers, and e-mail address to 690 ISS/PI-T. Submit updates when changes are required. Ensure the appointed unit officer is from a technical career field and have a working knowledge of electronics.

3.2. Unit TEMPEST Officer. The TEMPEST officer:

3.2.1. Is the focal point for all unit TEMPEST matters.

3.2.2. Keeps a reference library of TEMPEST publications. As a minimum, the library must contain NSTISSAM TEMPEST/2-95, AFI 33-203, AFSSI 7010 (S), AFSSM 7011, Inspectable Space Determination Message or the Zoning Report, and AIAI 33-203; include DoD 5105.21-M-1, if it is a DIA SCIF.

3.2.3. Attends Air Education and Training Command (AETC) course L3OZR33S3A-013, *TEMPEST Fundamentals*, or biannually, the TEMPEST workshop given by the AIA TEMPEST officer.

3.2.4. Reviews TEMPEST documents and keeps current with TEMPEST data applicable to the unit's TEMPEST security. The current AF EMSEC program is on the NIPRNET, worldwide web, at http:/ /www.afca.scott.af.mil/gc/gci.

3.2.5. Reviews Table of Allowance documents ensuring TEMPEST is considered for all applicable equipment. Obtain approval for any TEMPEST equipment based on approved programs or surveys.

3.2.6. Is knowledgeable of all unit programs on installing or removing equipment or systems which process national security information electrically and ensures TEMPEST integrity is maintained.

3.2.7. Requests approval for the following items from the SCIF accreditation authority:

3.2.7.1. RF transmitters.

3.2.7.2. Commercial television systems.

3.2.7.3. Dual mode facsimile systems.

3.2.7.4. Audio systems (with lines that exit the SCIF boundary).

3.2.7.5. Protected Distribution Systems (PDS).

3.2.7.6. Multilevel systems.

NOTE:

Use DoD 5105.21-M-1, Appendix J, if a DIA SCIF. Send a letter to NSA/C312, 9800 Savage Rd (SAB3), Fort Meade MD 20755-6706 if a NSA SCIF.

3.2.8. Inspects new or modified equipment, systems or facility installations, and ensures discrepancies are corrected before activation. Signs the AF Form 1261, *Command, Control, Communications and Computer Systems Acceptance Certificate*, and AF Form 332 work as applicable.

3.2.9. Annually in September, inspects local facilities for RED/BLACK compliance using AIACL 33-1 modified to fit the Inspectable Space Determination (ISD) and any other local requirements. Prepares separate checklists for mission areas and office areas. Send a copy of completed checklists to 690 ISS/PI-T by 31 October, maintain a copy for office files until superseded by the next annual inspection.

3.2.10. Maintains records of inspections that identify TEMPEST discrepancies and corrective actions in unit files until all discrepancies are corrected. Ensures actions for correcting TEMPEST discrepancies are reported quarterly to 690 ISS/PI-T.

NOTE:

Units under a Support Agreement Program submit a RED/BLACK checklist for equipment AIA installs or maintains. An Emission Security (EMSEC) inspection done by the host base is sufficient.

3.2.11. Monitors and guides local self-help activities for TEMPEST compliance.

3.2.12. Guides and assists local staff elements on TEMPEST matters and requests assistance from the AIA TEMPEST officer as required.

3.2.13. Establishes a unit TEMPEST education program through the Security, Training, Education and Motivation (STEM) council.

3.2.14. Submits TEMPEST testing requirements or requests for evaluations to 690 ISS/PI-T as required.

Chapter 4

PERSONNEL

4.1. Documentation. All AIA personnel who prepare or process C4 Systems Requirements Document (CSRD), Statements of Work (SOW) or requirements, Operational Required Document (ORD), operations plans, policies, directives, self-help installation projects, and Communication-Computer Systems Programs Plans (CSPP) that process classified information will ensure TEMPEST is considered. This requirement also applies to engineering proposals that result in operating, procuring, maintaining, or installing AIA equipment and systems, which process National Security Information. Contact 690 ISS/ PI-T for appropriate TEMPEST criterions and a standard statement.

4.2. Self-Help Projects. The unit TEMPEST officer inspects all unit personnel self-help projects prior to operation, if it processes classified or if it is operating in a SCIF.

4.3. When Using Electronic Equipment. All personnel will fully comply with TEMPEST policies and operating procedures when using electronic equipment that processes national security information.

FRANK B. RICHARDSON JR., Colonel, USAF
Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES, ACRONYMS AND ABBREVIATIONS, AND TERMS

References

AIR FORCE

AFI 33-203, Emission Security

AFMAN 33-272, (U) Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (S)

AFSSI 7010, (U) Emission Security Assessment (S). To be AFMAN 33-214, Vol. 1

AFSSM 7011, Emission Security Countermeasures Review. To be AFMAN 33-214, Vol. 2.

DEPARTMENT OF DEFENSE

DoD 5105.21-M-1, *Sensitive Compartmented Information Administrative Security Manual*

DIRECTOR CENTRAL INTELLIGENCE DIRECTIVE (DCID)

DCID 1/21, *Implementation Manuel for Physical Security Standards for Sensitive Compartmented Information Facilities*

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

NSA/CSS Cir. No. 100-1, (U) *NSA/CSS Secure Telephone System* (C)

NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEM SECURITY COMMITTEE (NSTISSC)

NSTISSAM TEMPEST/1-95, *Shielded Enclosures*

NSTISSAM TEMPEST/2-95, (U//FOUO) *RED/BLACK Installation Guidance*

NSTISSI No. 4002, (U) *Classification Guide for COMSEC Information* (S)

NSTISSI No. 7000, (U) *TEMPEST Countermeasures for Facilities* (C)

NSTISSI No. 7001, (U) *NONSTOP Countermeasures* (S)

NSTISSI No. 7002, (U) *TEMPEST Glossary* (S)

NSTISSI No. 7003, *Protected Distribution System (PDS)*

TELEPHONE SECURITY GROUP

TSG 1, *Introduction to Telephone Security*

TSG 6, *TSG Approved Equipment*

AIR INTELLIGENCE AGENCY

AIACL 33-1, *Management of TEMPEST Inspections in Air Intelligence Agency Sensitive Compartmented Information Facilities*

AIACL 33-2, *Management of TEMPEST Inspections for Shielded Enclosures*

Acronyms and Abbreviations

AETC--Air Education and Training Command

AFCA--Air Force Communications Agency

AFCOMSEC--Air Force Communications Security (used on forms)

AFI--Air Force Instruction

AFIWC--Air Force Information Warfare Center

AFSSI--Air Force Systems Security Instruction

AFSSM--Air Force Systems Security Memorandum

AIA--Air Intelligence Agency

ANG--Air National Guard

C4--Command, Control, Communications, and Computers

CE--Compromising Emanations

COMSEC--Communications Security

CSRD--C4 Systems Requirements Document

CSRD--Communication System Requirements Document

CTTA--Certified TEMPEST Technical Authority

DAA--Designated Approving Authority

DIA--Defense Intelligence Agency

DoD--Department of Defense

EMSEC--Emission Security

IS--Inspectable Space

ISD--Inspectable Space Determination

IP--Information Protection

MAJCOM--Major Command

MB--Maintenance Bulletin

NSI--National Security Information

NSA--National Security Agency

OPR--Office of Primary Responsibility

ORD--Operational Requirements Document

PDS--Protected Distribution System

PIPR--Plant In Place Records

RF--Radio Frequency

SCI--Sensitive Compartmented Information

SCIF--Sensitive Compartmented Information Facility

SPECAT--Special Category

TAD--Telephone Answering Device

TSG--Telephone Security Group

USAF--United States Air Force

Terms

Certified TEMPEST Technical Authority (CTTA). An experienced, technically qualified government employee who has met established certification requirements according to National Security Telecommunications and Information Systems Security Committee-approved criteria and appointed by a United States Government department or agency to fulfill CTTA responsibilities.

Collateral Information. All national security information classified under the provisions of an executive order, for which special community systems of compartments (e.g., Sensitive Compartmented Information) are not formally established.

Compromising Emanation. Unintentional signal that, if intercepted and analyzed, would disclose the information transferred, received, handled, or otherwise processed by any information-processing equipment.

Countermeasures. 1. That form of military science that by the employment of devices and, or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. 2. Any action, device, procedure, technique, or other means that reduces the vulnerability of an automated information system.

Countermeasures Review. A technical evaluation of a facility to identify the inspectable space, the required countermeasures, and the most cost-effective way to apply required countermeasures.

Emanation. Unintended signals or noise appearing external to an equipment.

Emission Security (EMSEC). The protection resulting from all measures taken to deny unauthorized persons information of value that might be derived from NONSTOP and HIJACK intercepts and the interception and analysis of compromising emanations from crypto-equipment, information systems, and telecommunications systems.

Facility. 1. A real-property entity consisting of one or more of the following: a building; a structure; a utility system, pavement, and underlying land.

2. A physically definable area which contains classified national security information-processing equipment.

Hazard. A measure of both the existence and the compromising nature of an emanation. Hazards exist if, and only if compromising emanations are detectable beyond the inspectable space.

HIJACK. The definition of HIJACK is classified (see AFSSI 7010(S)).

Information Systems. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information.

Inspectable Space. The 3-dimensional space surrounding equipment that processes classified national security or sensitive information within which TEMPEST exploitation is not considered practical or where legal authority to identify or remove a potential TEMPEST exploitation exists.

Labeling. Labeling consist of a tag identifying the signal on the cable in accordance with AIAI 33-203.

Marking. Marking consist of a one inch wide color band around a cable to identify the level of classification on the cable.

National Security Information. Information that has been determined, pursuant to Executive Order 12958, Classified National Security Information, April 17, 1995, or any predecessor order, to require protection against unauthorized disclosure, and is so designated.

NONSTOP. The definition of NONSTOP is classified (see AFSSI 7010(S)).

RED and BLACK Concept. Separation of electrical and electronic circuits, components, equipment, and systems that handle classified plain text (RED) information in electrical signal form from those which handle unclassified (BLACK) information in the same form.

TEMPEST. An unclassified term referring to technical investigations for compromising emanations from electrically operated processing equipment; these investigations are conducted in support of emission security.

TEMPEST-Certified Equipment. Systems or equipment that were certified within the requirements of the effective edition of NSTISSAM TEMPEST/1-92, Level I, or TEMPEST specifications as determined by the department or agency concerned.

Attachment 2

INSTALLATION CRITERIONS

A2.1. Introduction.

A2.1.1. Scope. The installation criterions apply to all Air Intelligence Agency (AIA) activities and components including telecommunications centers which support these activities. At AIA activities where the unit is a tenant to another organization, enforce these guidelines to the fullest extent the host base allows.

A2.1.2. Purpose. This guidance is intended to promulgate, clarify, and augment national and United States Air Force installation guidance. When this document and NSTISSAM TEMPEST/2-95 or AFSSI 7011 conflict, contact 690 ISS/PI-T for guidance.

A2.1.3. Background:

A2.1.3.1. In the past, TEMPEST criterions dictated ferrous conduit and ducts which enclosed both RED and BLACK cabling. Accordingly, operations floors and computer centers were a maze of special plumbing which became an installer's nightmare.

A2.1.3.2. AIA could not fully implement the above guidelines because of the nature of our large mission areas. In theory, all of the system wiring from the receiver outputs, through all processors, recording and printing devices would be RED and all antenna cables would be BLACK. One glance inside an Air Intelligence Agency signals intelligence (SIGINT) facility would indicate the impracticality of separately enclosing the hundreds of antenna cables, in conduit or duct, throughout their many diverse routings. Accordingly, AIA established a policy that the (RF) multicouplers, preamps, etc., satisfactorily acted as isolation devices between RED equipment and the BLACK antennas. (These devices attenuate conducted emanations or stray radiation in the reverse mode, that is, escaping the antennas.) Periodic TEMPEST testing of entire field stations over the years has confirmed this theory and no compromising emanations have been found beyond the operations building. Where raised floors are used, AIA implemented a requirement to place all RED cables under the raised floor, and to install all Black cables overhead to the extent possible.

A2.1.3.3. With the change in the world's threat situation and the proliferation of commercial-off-the-shelf stand-alone personal computers in the office environment and in AIA's large mission areas, previous guidance was no longer practical.

A2.1.3.4. TEMPEST standards have changed in general according to NSTISSAM TEMPEST/ 2-95 and AFSSI 7011. TEMPEST requirements are now based on the threat at the location, inspectable space, type of equipment, physical control, etc.

A2.1.3.5. The current AIA TEMPEST policy is based on good engineering and installation practices and all signal lines having one overall shield. Although the term "good engineering and installation practices" is nebulous, it is the basis of NSTISSAM TEMPEST/2-95, MIL-HDBK-419A, and AFSSI 7011 which attempts to define and explain these practices. For clarity, consider good engineering and installation practices as those which provide neat, clean, and orderly installations; protect cabling from inadvertent physical damage; provide wireline accountability; and enhance the electronic security of AIA activities.

A2.1.3.6. To conform to these practices, AIA developed a policy of marking cables and running all SCI cables under a raised floor and all BLACK cables above the false ceiling to the maximum extent possible. Place BLACK cables under the raised floor and other than BLACK cables above the false ceiling in the conduit. Mark cables according to paragraph A2.4, and meet the separation requirements of NSTISSAM TEMPEST/2-95. The AIA TEMPEST officer must approve any deviations from this policy for mission floors, computer floors, and communications centers. Guidance for specific installation standards for individual facilities is contained in NSTISSAM TEMPEST/2-95, AFSSI 7011, and this instruction.

A2.2. Signal Distribution and Installation:

A2.2.1. SCIF Cable Shielding Requirements. All metallic cables installed in a SCIF must have a minimum of one overall nonferrous shield (see NSTISSAM TEMPEST/2-95, section 6). If a copper cable does not have at least one overall nonferrous shield, install the signal lines in conduit or duct.

A2.2.1.1. Fiber Optic Cable. A fiber optic cable is the recommended method of signal distribution in AIA SCIFs. It is AIA guidance to migrate circuits that lend themselves to fiber optic cables to do so. This guidance is based on TEMPEST requirements and future requirements for greater data rate requiring larger bandwidths. It also does not have an electromagnetic field that would cause a TEMPEST problem and does not require any shielding or separation.

A2.2.1.2. Analog Signal Cables. Cables equipped with foil-type shields that generally provide adequate shielding for analog signals.

A2.2.1.3. Digital Signal Cables. Cables carrying digital data signals require a foil or braided shield that provide a minimum coverage of 90 percent. Connect the shields to the RF-tight EMI (electromagnetic interference) connectors on each end so that a 360-degree continuity between the cable shield and the connector is achieved.

A2.3. Distribution System Requirements:

A2.3.1. Keep unclassified, collateral, and SCI-signal lines separate from each other; that is, not in the same cable bundle or grouped together, see NSTISSAM TEMPEST/2-95, paragraph 6.8.

A2.3.2. Where required, install shielded copper signal lines and fiber optic lines in a nonmetallic or open distribution system.

A2.3.3. Terminate cable shields directly to the signal ground bus on the Intermediate Distribution Frame (IDF) and at the terminal block.

A2.3.4. Do not use cable shields as intentional current carrying conductors or as signal returns.

A2.3.5. Remove all abandoned and unused cables and conduit unless specifically programmed for use at a later date.

A2.3.6. Wireline separation distances for individual locations are found in your Inspectable Space Determination letter or message and NSTISSAM TEMPEST/2-95, section 3.

A2.4. Identification and Marking Requirements:

A2.4.1. The primary purpose of marking cables is to prevent accidental cross connections that could lead to a security incident. Marking consist of a 1-inch wide color band around the cable. Use

BLACK for unclassified, RED for collateral classified, and yellow for SCI. Different color connectors may also be used for marking. Marking and labeling is also a requirement of DCID 1/21, annex G, and NSTISSAM TEMPEST/2-95, paragraphs 4.4.2.2 and 4.5.

A2.4.2. To standardize marking, control placement of signal lines and maintain an accountability of the signal lines between systems, and mark and label all signal lines at both ends according to AIAH 33-102, **Engineering and Installation Standard**, attachment 1, drawing number 99-01-024. AIAH 33-102 is available for download at the AIAWeb site, www.aiaweb.aia.af.mil/products. All AIA units are responsible for adhering to this standard.

A2.4.3. Exceptions:

A2.4.3.1. The above policy applies to lines that run between different racks, hubs, switches, patch panels, etc. Internal lines do not require marking.

A2.4.3.2. Cables under the raised floor carrying other than SCI information require marking. SCI cables under a raised floor do not require marking (see paragraph A2.1.3.6).

A2.4.3.3. The LADYLOVE operations area will continue to follow the LADYLOVE site Installation Standard.

A2.4.3.4. Other site exceptions are determined on a case-by-case bases and are to be approved by the AIA TEMPEST Officer, 690 ISS/PI-T.

A2.4.4. Mark all cables entering or leaving systems or racks containing equipment of multilevel classifications, with the appropriate colored tape, regardless of where these systems or racks are installed.

A2.4.5. Mark duct or conduit capable of carrying more then 1 signal line with 1-inch tape approximately every 10 feet and upon entering and exiting a wall or ceiling.

A2.4.6. Classification is determined by the level of information processed and the equipment is to be labeled with Standard Form 700 series labels. Internal cabling are identified in TO's (Technical Orders), MB's (Maintenance Bulletins), Commercial Manuals, or Part II of the PIPRs (Plant in Place Records).

A2.4.7. Typically, office and administrative work spaces have equipment and systems (telephone, fax, computer, etc) that are classified at various levels. Mark cables in the office and administrative areas with the appropriate colored tape.

A2.5. Patch Panel Requirements. See NSTISSNAM TEMPEST/2-95, paragraph 4.5.2 and section 6. The requirement to prevent inadvertent cross patching are met in several ways.

A2.5.1. Use of Different Style Connectors. For fiber optic connectors, use the following:

A2.5.1.1. ST connectors--bayonet type for SCI lines.

A2.5.1.2. FC type connectors--screw on type for classified collateral lines.

A2.5.1.3. SC connectors--square type for unclassified or BLACK lines.

A2.5.2. Separation. Physical separation by a distance which would eliminate the possibility of cross patching.

A2.5.3. Software. Different software protocol for each level of classified information that will not allow interface with other levels.

A2.6. Separation Requirements:

A2.6.1. Since TEMPEST requirements are based on the location, inspectable space, type of equipment, physical control, etcetera; each unit has different installation criterions. The unit TEMPEST officer finds criterions particular to their circumstances according to NSTISSAM TEMPEST/2-95 and as identified in their Inspectable Space Determination (ISD). The Accreditation Authority (Defense Intelligence Agency [DIA] and the National Security Agency [NSA]) provided the ISD to the unit in a message or letter. Keep this letter or message on file.

A2.6.2. According to national policy, the separation distances when used in a SCIF are based on signal lined having one overall shield and are to be used as a minimum. It is AIA's policy to maintain 50 centimeters or 20 inches separation between any red processor and black equipment or cable to ensure there is not any physical contact or mutual conduction that would cause a hazard. If the separation requirements are not met, contact the AIA TEMPEST officer.

A2.6.3. A CTTA may modify this requirement depending on location and, or threat.

A2.7. Filters:

A2.7.1. Generally, power line filters are not required for AIA facilities in the CONUS.

A2.7.2. For the facilities that power line filters are considered, if sufficient physical security is maintained over the power lines to a point where the product of the currents and voltage exceed 100 KVA, then this will generally be sufficient. The SCIF Accreditation Authority (DIA or NSA) will specify power line filter requirements in the ISD.

A2.7.3. Signal line filters are required on signal lines exiting the inspectable space on a case-by-case basis. The SCIF Accreditation Authority (DIA or NSA) will specify the filter requirements in the ISD.

A2.8. Protected Distribution Systems (PDS). The SCIF accreditation authority (DIA or NSA) approval is obtained to use a new PDS or to modify an existing PDS, before system installation or modification begins. For DIA SCIFs, see DoD S-5105.21-M-1, Appendix J. For NSA SCIFs, send a letter to NSA/ C312, 9800 Savage Rd (SAB3), Fort Meade MD 20755-6706. Use NSTISSI No. 7003 or AFSSI 3030 for installation requirements.

A2.9. Isolation Requirements. Consider as a means of escape for classified information, service lines such as water lines, sewer lines, steam pipes, and any other metallic structures which service the secure area. The SCIF Accreditation Authority will specify the requirements in the ISD.

Attachment 3

VIDEO EQUIPMENT

A3.1. Classified. Install secure video equipment (VTC, JWICS, etc.) as a red processor according to the installation requirements of NSTISSAM TEMPEST/2-95.

A3.2. Unclassified:

A3.2.1. Install video equipment in break rooms and other areas where classified information is not discussed or electronically processed. Use it strictly for the convenience of unit personnel. **Do not** play classified video tapes on unclassified equipment.

A3.2.2. Cable television brought into the SCIF area is black equipment. Install cable televisions according to the requirements of NSTISSAM TEMPEST/2-95. This applies to television receivers and associated signal lines.

A3.2.3. Television receivers within the SCIF for cable must have the incoming antenna or cable service isolated to ensure TEMPEST and technical security are maintained. See NSTISSSAM TEMPEST/2-95, paragraph 4.9.6 for further details. A VCR (video cassette recorder) is not an acceptable isolation device.

A3.2.4. Contact a CTTA for television receivers within the SCIF for reception of local RF transmission.

A3.2.5. The system must be approved by the SCIF accreditation authority (DIA or NSA). Use the format in DoD 5105.21-M-1 for DIA SCIFs and send a letter to NSA/C312, 9800 Savage Rd (SAB3), Fort Meade MD 20755-6706 if a NSA SCIF.

Attachment 4

SECURE VOICE EQUIPMENT

A4.1. Secure Telecommunications. A STU-III or Secure Terminal Equipment (STE) is considered a black processor and should be installed as an administrative telephone.

A4.1.1. When a STU-III/STE is connected to a secure fax, computer, or some other classified processor, follow the guidance in NSTISSAM TEMPEST/2-95, paragraph 5.5.

A4.1.2. Single line STU-III/STEs may be used in SCIFs without additional protection. Plug jacks and specialized ringers are not required.

A4.1.3. Multiline models may be used in SCIFs under the following conditions.

A4.1.3.1. Common ringer is used.

A4.1.3.2. All components and wires of the Key System Unit (KSU) are contained within the SCIF. If a telephone instrument connected to the KSU is located outside the SCIF, contact a CTTA for appropriate countermeasures.

NOTE:

KSU approved for SCIFs are listed in the Telephone Security Group (TSG) 6, Guidelines for Computerized Telephone Systems (CTS). See DCID 1/21, annex G for requirements.

A4.1.4. Do not use STU-III/STEs with the speaker phone feature in a SCIF unless retrofitted to disconnect the console microphone and speaker. Your CSA may grant waivers for conference rooms or special offices.

A4.2. NSTS. NSA/CSS Circular No. 100-1 provides specific installation guidance for the NSTS.

A4.3. Audio Security. Avoid simultaneous use of secure voice equipment and BLACK telephone equipment. Care must also be taken to preclude inadvertent disclosure of SCI background conversations or data when using collateral secure voice terminals within an SCI area.

Attachment 5

ADMINISTRATIVE TELEPHONES

A5.1. System and Equipment Installation Requirements:

A5.1.1. DCID 1/21, Annex G, outlines requirements for telephone equipment and its installation in Sensitive Compartmented Intelligence Facilities (SCIF).

A5.1.2. The Telephone Security Group (TSG) published an Approved Equipment List, TSG Standard 6, *Computerized Telephone Systems*.

A5.1.3. All components of the telephone system, Key Telephone System or Computerized Private Branch Exchange, serving AIA facilities is wholly contained within the controlled area of the SCIF. Telephone lines which egress the facility are looked at on a case-by-case basis by a CTTA. US citizens who have appropriate security clearances have limited access to such equipment.

A5.1.4. See DCID 1/21, Annex D, for use of cordless and cellular telephones in AIA SCIFs.

A5.2. Separation Criterions:

A5.2.1. All administrative BLACK telephones are considered black processors and are to meet the installation requirements of NSTISSAM TEMPEST/2-95 or AFSSI 7011.

A5.2.2. It is AIA's policy to maintain a minimum separation of 20 inches or 50 centimeters between BLACK telephone instruments and any RED processor. Contact the AIA TEMPEST officer if you cannot achieve this separation.

A5.2.3. Black administrative telephones are to be kept at least 2 meters from any equipment on mission floors or in computer and communications centers.

A5.2.4. Avoid black telephone lines on mission floors and computer and communications centers. If the telephone lines are routed under the raised floor with RED cables, totally encase the phone lines in ferrous conduit or braided shielded cable. 690 ISS/PI-T must approve installation of BLACK signal lines under a raised floor.

A5.3. Grounding and Filtering Requirements:

A5.3.1. Ground all spare telephone wires and cable shields to a ground point established at the telephone filter panel or to the equal potential ground.

A5.3.2. Remove all abandoned cables and conduits unless specifically programmed for use at a later date.

A5.3.3. Do not filter or isolate BLACK telephone lines exiting the SCIF unless specified by a CTTA. If filtering is needed, a digital switch or a fiber optic line may provide sufficient protection.

A5.4. Prohibited Equipment. Speakerphones, headsets, and acoustic coupled equipment are generally prohibited, but may be used if prior approval has been granted by the Accreditation Authority according to DCID 1/21, Annex G.

A5.5. Policy. This policy is in consonance with telephone security policies established by Air Force Office of Special Investigation (AFOSI) and the Defense Intelligence Agency (DIA) and will remain in

effect until further notice. Please ensure your local telephone installation and planning personnel are aware of and implement this policy.

Attachment 6

ENTERTAINMENT AND PUBLIC ADDRESS SYSTEMS

A6.1. Comfort Music:

A6.1.1. AM, FM radios or audio amplifiers and associated equipment are used to provide entertainment or public address capabilities in areas under AIA's security cognizance.

A6.1.2. The office manager uses their discretion in limiting the number of radios in the area to prevent excessive noise.

A6.1.3. Tape recorders or combination radio receivers and tape recorders are prohibited. Install a tape player if there is a requirement for a continuous music source. Use a tape recorder as a tape player if its recording capability is disabled and, or disconnected.

A6.1.4. Install the systems components, that is; receivers, amplifiers, and speakers within the SCIF's confines. Install extension speakers at entry control points (ECP), outside the building, or in any area within the same physically controlled (fenced) area where people have at least a SECRET clearance. Contact a CTTA if a signal line exit the controlled area.

A6.1.5. The system is considered a black processor and is to be installed according to NSTISSAM TEMPEST/2-95 or AFSSI 7011. Use shielded cable throughout the system.

NOTE:

Mark antenna or speaker cables with labels that identify as music, television, or public address system cable. Run these cables above a false ceiling.

A6.1.6. Microphones of some systems are used to provide unclassified public address announcements (such as fire, disaster preparedness, etc.). Establish local OPSEC and COMSEC procedures for use.

A6.2. Cover Music. This subject is covered separately in DCID 1/21, Annex E. Refer to this document for further details.

A6.3. Television Receivers. See Attachment 3.

Attachment 7

FIBER OPTIC CABLE

A7.1. Method of Signal Distribution. Fiber optic cable is the recommended method of signal distribution in AIA SCIFs. It is guidance at the Air Intelligence Agency (AIA) to migrate circuits that lend themselves to fiber optic cable to do so. This is based on TEMPEST requirements and future requirements for greater data rates requiring larger bandwidths. It also does not have an electromagnetic field that would cause a TEMPEST problem and does not require any shielding.

A7.2. General. A fiber optic system converts an electrical signal to an optical signal, transmits the signal through an optical cable and reconverts the signal to electrical form at the other end of the fiber. Optical systems have several significant advantages over conventional cables when used to transmit RED clear text National Security Information (NSI) within AIA controlled areas. Fiber optic cables that have no metallic content do not conduct extraneous signals and are unaffected by electromagnetic fields. They are not subject to crosstalk, ground loop problem, or the transmission of common mode signals.

A7.3. Applications. Fiber optic systems that have no metallic content can be used to prevent the unintentional transmission of RED information outside the controlled space because they do not create electromagnetic fields which could be induced on the BLACK fortuitous conductors. A BLACK fiber optic cable may exit a RED area without further filtering or isolation. Steps should be taken to prevent RED contamination of the BLACK information before conversion to optical form. RED fiber optic cables may be used to traverse BLACK areas when Protected Distribution System (PDS) criterions are met.

A7.4. RED Fiber Optic Cable Separation. RED fiber optic cables need not comply with the RED/ BLACK separation requirements of NSTISSAM TEMPEST/2-95 or AFSSM 7011.

A7.5. Cable Strengthening Member. The strengthening member included in some multifiber cables may contain embedded wires or mesh. ***Note:*** Any conductive component in the cable can act as fortuitous conductors. For this reason, do not use fiber optic cables with metal or conductive material that egresses AIA facilities. Use of this type of cable external to AIA SCIFs will be addressed on a case by case basis.

A7.6. Multifiber Cables. Do not transmit RED and BLACK information on separate fibers within the same multifiber cable. Use separate cables and distribution systems with appropriate markings. Use separate fiber optic cables for each classification level (Collateral and SCI) of RED information that is processed.

A7.7. Common Mode Signal Rejection. Common mode rejection is a measure of how well an electronic device ignores a signal that appears simultaneously and in phase at both the input and output terminals. A fiber optic system with the source and detector powered from different power supplies or amplifiers will eliminate all common mode signals.

A7.8. Fiber Optic Circuits. Fiber optic cable that has no metallic content exhibits no electromagnetic radiation characteristics; however, it is possible to damage or tap the optical fiber. Therefore, the fiber requires physical protection against damage and tampering.

A7.9. RED Fiber Optic Cable Marking. Mark all RED fiber optic cables or their distribution system according to 668 LS standard drawing number 99-01-024 and attachment 2.

A7.10. Fiber Optic Connectors. See AIAI33-203, attachment 2, paragraph A2.5.1.1.

A7.11. Fiber Optic Converters. These devices serve as modems which convert the electromagnetic signals to light for transmission on fiber optic cables. Install as any other RED or BLACK equipment.

Attachment 8

TACTICAL EQUIPMENT

A8.1. References. See NSTISSAM TEMPEST/2-95 or AFSSI 7011 for Transportable Systems in a Tactical Environment.

A8.2. RED/BLACK Inspections. Use AIACL 33-1 and modify locally according to NSTISSAM TEMPEST/2-95 or AFSSI 7011 to perform RED/BLACK inspections on Tactical systems equipment. These systems are inspected annually or after a deployment, whichever comes first.

A8.3. Tactical Systems. Tactical systems such as Contingency Airborne Reconnaissance System are fully deployable, self-contained systems and are housed in a shielded enclosure. These shielded enclosures are inspected annually or after the system is moved, whichever comes first. Use AIACL 33-2 for this inspection.

A8.4. Transmitters. Transmitters in a Transportable Systems not meeting the installation requirements of NSTISSAM TEMPEST/2-95 are required to be evaluated by a CTTA according to NSTISSI 7001 and meet the requirements of NACSEM 5112.

A8.5. TEMPEST in the Airborne Environment. See NSTISSAM TEMPEST/2-95, section 9, for unique aircraft operations and installation.

A8.6. Aircraft Testing. All aircraft carrying AIA equipment are tested according to NACSEM 5112 for airborne system procurements and modifications unless otherwise specified by a CTTA.

Attachment 9

SHIELDED ENCLOSURES

A9.1. General. The use of shielded enclosures and shielding methods must be based on the results of an evaluation performed according to NSTISSI No. 7000. The evaluation must be conducted or validated by the cognizant CTTA. Shielded enclosures are to meet the requirements of NSTISSAM TEMPEST/1-95.

A9.2. Alternative Countermeasure. It is important to realize that shielded enclosures are only used when all other countermeasures are impractical or more costly. It is imperative that the CTTA be involved so TEMPEST alternatives or countermeasures are considered before a shielded enclosure, wall, or building shielding is used. Contact the AIA TEMPEST officer before any shielding is installed.

A9.3. Inspections. Shielded enclosures are to be inspected annually using AIACL 33-2.

Attachment 10

GROUND MAINTENANCE

A10.1. Ground System Test. The purpose of system ground test is to check each ground plate and its connection to the under floor ground grid against all other parallel ground circuits throughout the equipment facility. In effect, each ground plate is tested against a (theoretically) near-perfect ground, formed by all other paths plus that provided by building or antenna field ground.

A10.2. Ground Plates. Accomplish testing at all ground plates on the interior of external walls and columns. Measure value at each ground plate in the fractional ohm range (i.e., approximately 1/10 ohm) at the AN/FLR-9 stations with a complete ground grid under the concrete floor. At non-AN/FLR-9 stations and other facilities without a complete under floor grid (i.e., separate clusters of ground rods only), the measured value will likely be in the low ohm range (i.e., 1 to 5 ohms).

A10.3. Initial Check. Accomplish the initial check every 90 days for 1 year to develop a standard against which to compare future measurements. After initial measurements, accomplish periodic testing every 21 months and upon completion of major project upgrades. Erratic readings or problem ground connections should be checked at more frequent intervals.

A10.4. Ground Checks. Ground checks are accomplished using an appropriate test instrument such as a Fluke meter model 8100, a Vibroground model 251, or equivalent.

A10.5. Ground Checking Responsibilities. Responsibility for the maintenance of exterior grounds falls under the purview of BCE, AFI 32-1065, *Grounding Systems*. However, the responsibility for checking and validating operations floor and computer centers ground connections rests with unit LG and is also to be done according to AFI 32-1065.

A10.6. Ground Check Files. Log in results of the initial and periodic readings on a locally prepared chart specifically tailored to each site's requirements. Design the chart to easily identify fluctuations in readings over a period of time and is to be kept on file.

Attachment 11

RADIO FREQUENCY DEVICES

A11.1. Purpose. Radio frequency (RF)-based devices and systems pose a particularly significant TEMPEST hazard if not installed using good engineering practices. Devices that fall under these installation and engineering guidance are radio transmitters, receivers, land mobile radios, receive and transmit pagers, cellular telephones, wireless microphones, cordless telephones, etc. These devices are generally prohibited in a SCIF. See DCID 1/21, Annex D, for exceptions.

A11.2. Radio Transmitters. Radio transmitters are inherently BLACK equipment; however, they produce a RF signal that can introduce problems. To preclude these problems, special attention must be paid to the installation.

A11.2.1. It is mandatory to locate the transmitter and antenna outside the RED equipment area, a minimum of three meters and as close as possible to the point the antenna cable penetrated the SCIF.

A11.2.2. The transmitter will not be powered from the same source as the RED equipment. As a minimum, it should have its own power source back to the SCIF main power panel.

A11.2.3. If the antenna cable exits the control space, ensure the RF cables are routed to or through the radio frequency multicouplers, power dividers, or other RF equipment for isolation and a ground.

A11.2.4. The system should have an exceptionally good path to earth ground.

A11.2.5. When control and signal lines exit the control space, consult a CTTA.

A11.3. Approval Authority. Approval to install a transmitter in a SCIF shall be obtained before system installation begins from the SCIF accreditation authority (DIA or NSA). Specific instructions are in DoD -5105.21-M-1, appendix J for DIA SCIFs or send a letter to NSA/C312, 9800 Savage Rd (SAB3), Fort Meade MD 20755-6706 if an NSA SCIF.

A11.4. Transportable Requirements. When the transmitter equipment is contained within a shelter or van, see NSTISSAM TEMPEST/2-95, section 7, or AFSSI 7011, Attachment 17.

Attachment 12

OFFICE EQUIPMENT

A12.1. Purpose. All telephones and telephone systems installed in AIA SCIFs must meet the requirements of DCID 1/21, Annex G.

A12.2. Telephone Answering Devices (TAD). TADs can be a Technical and, or TEMPEST security hazard. Therefore, precautions and prior CSA approval is required for a TAD.

A12.2.1. The TAD is used in a single occupant office, whereas the occupant has no one to answer their telephone or cannot forward the calls when they are absent. Other uses of a TAD are addressed on a case-by-case basis.

A12.2.2. Use the TAD model that does not have remote control capability; i.e., you cannot call in for your messages or have a remote room monitoring capability. As with any telephone equipment, the TAD is government-owned and -procured; no personal equipment is authorized.

A12.2.3. Install a TAD only with an administrative BLACK telephone or STU-III/STE, if appropriate. Separation of the TAD from other unclassified or classified information processing systems will be according to TEMPEST installation guidelines of NSTISSAM TEMPEST/2-95.

A12.2.4. Turn the TAD off when the user is available to answer the telephone.

A12.2.5. Classify the TAD recording media to the highest level of information being processed in the immediate area and protect to that level. When no longer needed or defective, destroy the recording media according to applicable procedures for destruction of classified media.

A12.2.6. Remove the recording media before performing any maintenance on the TAD.

A12.3. BLACK Computers. Unclassified computers, whether used strictly for unclassified processing or connected to the Internet, is considered BLACK equipment. Install unclassified computers according to NSTISSAM TEMPEST/2-95 or AFSSM 7011. They are also subject to all computer security measures.

A12.4. Problem Equipment. Electronic equipment pose a TEMPEST problem when entered into a SCIF. See DCID 1/21, Annex D, for guidance on equipment allowed in a SCIF.

A12.4.1. Electronic recording machines pose a TEMPEST problem because they may inadvertently pick up stray electromagnetic signals in the immediate area and record the data on recording media. The recording media, usually magnetic tape, must be classified to the highest level of information being processed in the immediate area. Destroy recording media according to applicable procedures for destruction of classified information.

A12.4.2. The introduction of receive only pagers and beepers are allowed in AIA SCIFs.

A12.5. Facsimile Terminals. See DIA 50-24, *Security Policy for Using Communications Equipment in a SCIF,* for operating instructions for facsimile machines in a SCIF. Install all facsimile machines according to NSTISSM TEMPEST/2-95.

A12.5.1. Single mode facsimiles no longer require a System Security Plan for secure or unsecure facsimile machines. However, facsimiles still require approval from the Information Systems Security Manager for operation within a SCIF.

A12.5.2. Approve dual mode terminals (classified and unclassified) by the SCIF Approval Authority (DIA or NSA).

A12.6. Other Office Equipment. Install BLACK facsimile terminals, microfiche readers, time stamps, and other office equipment which do not process information electrically, electro-mechanically, or electronically as BLACK equipment. Install typewriters and photostatic (Xerox) copiers as BLACK equipment, even though they are used to process classified information.

A12.7. Typewriters. Presently, typewriters are few and far in between and are rarely used to type classified information. Because of this typewriters are not considered a TEMPEST problem and do not require any additional protection.

A12.8. Microwave Ovens. Microwave ovens do not constitute a TEMPEST hazard if they are properly installed. Federal health and safety standards, as well as FCC standards, severely limit microwave emanations from these ovens. Also, the relatively low duty cycles limit TEMPEST vulnerability.

A12.9. Refrigerators, Coffeepots, Toasters. These items are not radiators and are not considered a TEMPEST hazard.

A12.10. Unclassified Area. The creation of a de facto unclassified area is advisable for all equipment not processing classified information. Use partitions, signs, and equipment labels to denote this area. See NSTISSAM TEMPEST/2-95, 4.3 and 4.9.